COMPARATIVE STUDY OF MULTIPLE BLACK HOLE ATTACKS SOLUTION METHODS IN MANET USING AODV ROUTING PROTOCOL

ELAHE FAZELDEHKORDI

A thesis submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014

This thesis is dedicated to my beloved parents for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to sincerely thank my lovely parents, **Behjat Kazemi** and **Manouchehr Fazel**, my lovely brothers **Peyman Fazel**, **Amin Fazel** and **Pouya Fazel**, my best friend **Akanbi Oluwatobi Ayodeji** and all friends for their endless love, support and encouragement. I could not have done it without you! There is no word I can find to thank you.

Next, I would like to express my heartfelt gratitude to my supervisor **Prof. Dr. Abdul Hanan Abdullah** and **Mr. Adnan Ahmed** for their constant support during this project. They inspired me greatly to work in this project. Their willingness to motivate me contributed tremendously to the success of this project. I have learned a lot from them and I could not have imagined having a better advisor and mentor for my Master study. Many thanks to all my lecturers, I will forever be grateful.

Besides, I would like to thank my examiners: **Dr. Mohammad Abdur Razzaque**, and **Dr. Ismail Fauzi Bin Isnin** for their patience and insightful comments.

Finally, I would like to thank Universiti Teknologi Malaysia for their kind cooperation.

ABSTRACT

Mobile Wireless Ad Hoc Networks (MANET) are non-centralized wireless networks that can be formulated without the need for any pre-existing infrastructure in which each node can act as a router. It must discover its local neighbours and through them it will communicate to nodes that are out of its transmission range. Various features like open medium, dynamic topology, lack of clear lines of defence, makes MANET vulnerable to security attacks. Ad hoc On-demand Distance Vector routing (AODV) is one of the best and popular routing algorithms. AODV is severely affected by well-known black hole attack in which a malicious node injects a faked route reply message that it has a fresh route to destination. In this thesis, MANET performance against single black hole attack has compared with its performance against multiple black hole attacks by using Intrusion Detection System (IDSAODV) routing protocol (Dokurer, 2006). The result are analysed using NS-2.35, through various network parameter bases: total drop packets, end to end delay, packet delivery ratio and routing request overhead. The results indicate IDSAODV solution method which is presented for single black hole attack before, can be used effectively for decreasing total drop packets and improving packet delivery ratio against multiple black hole attacks, also. But, the method doesn’t have significant effect for improving end to end delay and routing request overhead.

ABSTRAK

Rangkaian Tanpa Wayar Ad Hoc Bergerak (MANET) adalah rangkaian tanpa wayar tidak berpusat yang boleh dirumuskan tanpa memerlukan sebarang infrastruktur yang sedia ada dimana setiap nod boleh diguna sebagai penghala. Ia perlu mengetahui jiran-jiran setempat dan melaluinya ia boleh berkomunikasi dengan nod-nod yang luar dari lingkungan transmisinya. Pelbagai ciri-ciri seperti media terbuka, topologi dinamik, kekurangan pada garisan pertahanan, membuat MANET terdedah kepada serangan-serangan keselamatan. Penghala Vektor Jarak Ad-hoc atas Permintaan (AODV) adalah salah satu yang terbaik dan popular diantara algoritma-algoritma penghala. AODV terjejas dengan teruk oleh serangan lubang hitam yang terkenal dimana nod yang bahaya menyuntik mesej balas yang palsu yang mempunyai laluan yang segar kepada destinasinya. Di dalam kajian ini, prestasi MANET terhadap satu serangan lubang hitam telah disbanding dengan prestasinya terhadap serangan lubang hitam yang banyak dengan menggunakan protokol laluan (Dokurer, 2006) Sistem Pengesanan Pencerobohan (IDSAODV). Hasilnya dianalisis dengan menggunakan NS-2.35, menerusi pelbagai pengakalan parameter rangkaian: jumlah paket-paket yang jatuh, penangguhan hujung ke hujung, nisbah penghantaran paket dan permintaan penghala atas. Hasil menunjukkan bahawa kaedah penyelesaian IDSAODC yang telah dikemukakan sebelumnya dengan satu serangan lubang hitam, boleh digunakan dengan berkesan untuk menguranKan jumlah paket-paket yang jatuh dan mempertingkatkan nisbah penghantaran paket terhadap serangan lubang hitam yang banyak. Akan tetapi, kaedah ini tidak mempunyai kesan yang ketara dalam mempertingkatkan penangguhan hujung ke hujung dan permintaan laluan atas.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Mobile Ad-Hoc Networks are independent and non-centralized wireless techniques. MANETs involve mobile nodes which are free in shifting in and out in the network. Nodes are the techniques or gadgets i.e. cell phone, laptop computer, individual electronic support, MP3 gamer and pc that are playing the network and are mobile. These nodes can work like host/router or both at the similar time. They can type irrelevant topologies based on their connection with each other in the network. These nodes have the capability to set up them and because of their self-settings capability, they can be implemented quickly out of need to any infrastructure (Ullah and Rehman, 2010).

Security in Mobile Ad-Hoc Network is the most serious issue for the primary performance of network. The accessibility to network services, privacy and reliability of the details can be carried out by guaranteeing which protection problems have been met (Ullah and Rehman, 2010). MANETs generally is affected from protection attacks for the sake of its functions like open medium, modifying its topology dynamically, deficiency of main monitoring and control, cooperative methods and no obvious protection procedure (Ullah and Rehman, 2010). These aspects have modified the fight area scenario for the MANETs versus the protection risks.

Routing protocols have created that determine how routers communicate with each other and how to select routes between any two nodes on a computer network. In general, routing methods is one of the complicated and exciting analysis places. Many routing methods have been designed for MANETS, i.e. AODV, OLSR, DSR etc. (Ullah and Rehman, 2010).

AODV is one of the well-known On-Demand Routing techniques (Das et al., 2003). Some scientists (Deng et al., 2002, Ramaswamy et al., 2003) investigated on this routing protocol and discussed the weaknesses in Ad hoc routing protocols and the attacks which can be installed. Recording to a research carried out by (Usha and Bose, 2012) AODV technique is most unprotected versus the black hole attacks.

1.2 Problem Background

MANET is so much well-known due to the point which these networks are powerful, facilities less and scalable. Despite the truth of reputation of MANET, these networks are so much revealed to attacks (Lu et al., 2009, Ullah and Rehman, 2010). Wi-Fi hyperlinks also create the MANET more vulnerable to attacks which create it simpler for the enemy to go within the network and capture accessibility the continuous interaction. Different types of attacks have been examined in MANET and their impact on the network. Attack such as greyish opening, where the enemy node acts maliciously for enough time until the packages are decreased and then change to their regular actions. MANETs routing methods are also being utilized by the assailants by means of surging attack, which is done by the enemy either by using RREQ or details surging (Ullah and Rehman, 2010).

In any network, the sender wants its details to be sent as soon as possible in a protected and quick way, many assailants promote themselves to have the quickest and great data transfer usage available for the transmitting similarly in wormhole attack, and the enemy captures themselves in powerful ideal place in the network.

They create the use of their place i.e. they have quickest direction between the nodes (Mahajan et al., 2008, Shanthi et al., 2009). One of the most coming up problems in MANET is the restricted power supply, assailants take a benefit of this defect and attempts to keep the nodes conscious until all its power is missing and the node go into long lasting rest. Many other attacks MANET for instance jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been analyzed and revealed (Ullah and Rehman, 2010).

In black hole attack, a harmful node uses its routing technique to be able to promote itself for having the quickest direction to the place node or to the bundle it wants to identify. Furthermore, this aggressive node promotes its accessibility to clean tracks regardless of verifying its routing table. In this way enemy node regularly will have the provision in responding to the direction demand and thus identify the details bundle and maintain it (Ullah and Rehman, 2010).

Researchers have suggested alternatives to recognize and remove black hole nodes (Deng et al., 2002, Ramaswamy et al., 2003). Deng et al. (2002) suggested a remedy for personal dark gaps. But they have not regarded the supportive black hole attacks. As stated in their method, details about the next hop to place should be involved in the RREP bundle when any advanced node responses for RREQ. Then the resource node delivers a further demand (FREQ) to next hop of responded node and requests about the responded node and direction to the place. By using this technique we can recognize standing of the responded node only if the next hop is reliable. However, this remedy cannot avoid supportive black hole attacks on MANETs. For instance, if the next hop cooperates with the responded node, as well, the response for the FREQ will be basically “yes” for both concerns. Then the resource will believe in on next hop and deliver details through the responded node which is a black hole node.

Ramaswamy et al. (2003) suggested a remedy to protecting versus supportive black hole attacks. Also, they claimed that no models or performance assessments have been done. Therefore, this project focuses on assessment of the performance of the suggested plan in protecting versus the supportive black hole attack.

1.3 Problem Statement

Based on researches carried out by Sharma and Gupta (2009) shows that AODV greatly suffers from multiple black holes in terms of packet delivery ratio, drop packets, average end-to-end delay and route request overhead. Besides, the most common techniques used are inefficient in responding to multiple black hole attacks and just can prevent of single black hole attack (Lee et al., 2002, Deng et al., 2002, Sun et al., 2003). So little attention has been given examine and implementing existing methods for prevention of multiple black hole attacks. There is a need to analyze these methods on multiple black hole attacks. Therefore, this study will address the following questions:

i. How to detect single and multiple black hole attack?
ii. How to mitigate single black hole attack using the most efficient solution?
iii. How to mitigate multiple black hole attack using the methods in (ii)
iv. How to determine the efficiency of the solution used in black hole attack by comparing ids aodv with black hole aodv using the following metrics: packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead?

1.4 Purpose of Study

In this research, performance of one of the most efficient solutions for preventing single black hole attack in MANET using AODV routing protocol will be investigated in terms of packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead. Then will examine MANET performance under multiple black hole attacks with proposed solution. At the end of this investigation, it will be highlighted if the solution which shows good performance in terms of high packet delivery ratio, low packet loss percentage, low average end-to-end delay and reduce route request overhead for single black hole attack can also be useful face with multiple black hole attacks.

1.5 Project Objectives

There are four objectives for this project. They are:

i. To investigate the existing solutions for preventing single black hole attack in MANET using AODV routing protocol.

ii. To determine one of the efficient existing solutions above using four metrics: packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead.

iii. To implement the existed solution (IDSAODV (Dokurer, 2006) which has presented for single black hole attack before), for multiple black hole attacks.

iv. To compare the effects of above solution on MANET performance with single black hole attack and multiple black hole attacks.

1.6 Scope of Study

The scopes of this research are as follow:

i. The project will study the effects of multiple black hole attacks in MANET using (AODV Ad-Hoc on Demand Distance Vector) routing protocol.

ii. Analysis of solutions for preventing single black hole attack is taken into account.

iii. The impact of solutions for preventing multiple black hole attacks on the performance of MANET is evaluated, finding out if solutions for single black hole attack are also useful for multiple black hole attacks.

iv. Simulation will be done in NS-2.35 (Network Simulator).

v. Simulation will examine on MANET without black hole attack, MANET with 1 black hole node, MANET with 2 black hole nodes and MANET with 3 black hole nodes. And in each scenario will work on networks with 6 nodes, 20 nodes and 30 nodes separately.

vi. Simulation parameters will be obtained from authors of proposed solution (Arya and Jain, 2011, Ahmad et al., 2012).

vii. The measurements will be obtained using packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead.

1.7 The Significance of Study

Nowadays, there is an increasing need to preventing multiple black hole attacks due to the adverse effect they can have on their victims. Lots of work has been done on single black hole prevention using several techniques to achieve the same goal, but the question is if these techniques can be useful for multiple black hole attacks? This study evaluates the performance one of the most efficient of these techniques as regards to packet delivery ratio, packet loss percentage, average end-to-end delay and route request overhead for preventing of single black hole attack and multiple black hole attacks on MANET using AODV routing protocol by studying each of those metrics individually and will carry out by MANET performance with multiple black hole attacks under single black hole attack prevention solutions.

1.8 Organization of Report

The thesis consists of six chapters. Chapter one describes the introduction, background of the study, research objectives and questions, the scope of the study and its primary objectives. The second chapter reviews available and related literature on black hole attack detection. Chapter three describes the study methodology along with the appropriate framework for the study. Chapter four describes the effects of the single black hole and multiple black hole attacks on MANT performance. Chapter 5 discusses the implementation, result and analysis based on research framework. Finally, Chapter 6 concludes the thesis with a closing remark, recap of objectives, contribution and future work.

REFERENCES

Ahmad, Z., Manan, J.-L. A. and Jalil, K. A., 2012. Performance Evaluation On Modified Aodv Protocols. Applied Electromagnetics (Apace), 2012 IEEE Asia-Pacific Conference On, 2012. IEEE, 158-163.

Arunmozhi, S. and Venkataramani, Y., 2012. Black Hole Attack Detection And Performance Improvement In Mobile Ad-Hoc Network. *Information Security Journal: A Global Perspective,* 21**,** 150-158.

Arya, M. and Jain, Y. K., 2011. Grayhole Attack And Prevention In Mobile Adhoc Network. *International Journal Of Computer Applications,* 27.

Bakshi, A., Sharma, A. and Mishra, A., 2013. Significance Of Mobile Ad-Hoc Networks (Manets).

Begam, U. S. and Murugaboopathi, G., 2013. A Recent Secure Intrusion Detection System For Manets.

Bessire, M. L., 2006. System And Method For Ensuring The Availability Of A Storage System. Google Patents.

Bhardwaj, P. K., Sharma, S. and Dubey, V., 2012. Comparative Analysis Of Reactive And Proactive Protocol Of Mobile Ad-Hoc Network. *International Journal,* 4.

Bhattacharyya, A., Banerjee, A., Bose, D., Saha, H. N. and Bhattacharya, D., 2011. Different Types Of Attacks In Mobile Adhoc Network. *Arxiv Preprint Arxiv:1111.4090*.

Bhushan, B., Gupta, S. and Nagpal, C., 2013. Comparison Of On Demand Routing Protocols. *International Journal Of Information Technology,* 5.

Chavda, K. S. and Nimavat, A. V., 2013. Comparative Analysis Of Detection And Prevention Techniques Of Black Hole Attack In Aodv Routing Protocol Of Manet.

Cheng, H., 2012. Genetic Algorithms With Hyper-Mutation For Dynamic Load Balanced Clustering Problem In Mobile Ad Hoc Networks. Natural Computation (Icnc), 2012 Eighth International Conference On, 2012. IEEE, 1171-1176.

Chun, J., Shioura, A., Tien, T. M. and Tokuyama, T., 2013. A Unified View To Greedy Geometric Routing Algorithms In Ad Hoc Networks. *Algorithms For Sensor Systems.* Springer.

Dadhania, P. and Patel, S., 2013. Performance Evaluation Of Routing Protocol Like Aodv And Dsr Under Black Hole Attacks. *Performance Evaluation,* 3**,** 1487-1491.

Dangore, M. M. Y. and Sambare, M. S. S., 2013. A Survey On Detection Of Blackhole Attack Using Aodv Protocol In Manet.

Das, S. R., Belding-Royer, E. M. and Perkins, C. E., 2003. Ad Hoc On-Demand Distance Vector (Aodv) Routing.

Deng, H., Li, W. and Agrawal, D. P., 2002. Routing Security In Wireless Ad Hoc Networks. *Communications Magazine, Ieee,* 40**,** 70-75.

Dokurer, S., 2006. *Simulation Of Black Hole Attack In Wireless Ad-Hoc Networks,* Atılım University.

Gupta, N. and Shrivastava, M., 2013. An Evaluation Of Manet Routing Protocol. *International Journal*.

Hassnawi, L., Ahmad, R., Yahya, A., Aljunid, S. and Elshaikh, M., 2012. Performance Analysis Of Various Routing Protocols For Motorway Surveillance System Cameras' Network. *International Journal Of Computer Science,* 9.

Issariyakul, T., 2012. *Introduction To Network Simulator Ns2*, Springer Science+ Business Media.

Issariyakul, T. and Hossain, E., 2012. *An Introduction To Network Simulator Ns2*, Springer.

Jawandhiya, P. M., Ghonge, M. M., Ali, M. and Deshpande, J., 2010. A Survey Of Mobile Ad Hoc Network Attacks. *International Journal Of Engineering Science And Technology,* 2**,** 4063-4071.

Kaur, D. and Kumar, N., 2013. Comparative Analysis Of Aodv, Olsr, Tora, Dsr And Dsdv Routing Protocols In Mobile Ad-Hoc Networks. *International Journal,* 5.

Kaur, R. and Rai, M. K., 2012. A Novel Review On Routing Protocols In Manets. *Undergraduate Academic Research Journal (Uarj), Issn*, 2278-1129.

Koyama, A. and Suzuki, H., 2013. Real Object-Oriented Communication Method For Ad Hoc Networks. *Journal Of Computer And System Sciences*.

Lee, S., Han, B. and Shin, M., 2002. Robust Routing In Wireless Ad Hoc Networks. Parallel Processing Workshops, 2002. Proceedings. International Conference On, 2002. IEEE, 73-78.

Liu, W., Nishiyama, H., Ansari, N., Yang, J. and Kato, N., 2013. Cluster-Based Certificate Revocation With Vindication Capability For Mobile Ad Hoc Networks. *Parallel And Distributed Systems, IEEE Transactions On,* 24**,** 239-249.

Lu, S., Li, L., Lam, K.-Y. and Jia, L., 2009. Saodv: A Manet Routing Protocol That Can Withstand Black Hole Attack. Computational Intelligence And Security, 2009. Cis'09. International Conference On, 2009. Ieee, 421-425.

Mahajan, V., Natu, M. and Sethi, A., 2008. Analysis Of Wormhole Intrusion Attacks In Manets. Military Communications Conference, 2008. Milcom 2008. IEEE, 2008. IEEE, 1-7.

Menon, V. G., Johny, V., Tony, T. and Alias, E., 2013. Performance Analysis Of Traditional Topology Based Routing Protocols In Mobile Ad Hoc Networks. *International Journal Of Computer Science,* 2.

Mistry, N., Jinwala, D. C. and Zaveri, M., 2010. Improving Aodv Protocol Against Blackhole Attacks. Proceedings Of The International Multiconference Of Engineers And Computer Scientists, 2010. 17-19.

Murthy, C. S. R. and Manoj, B., 2004. *Ad Hoc Wireless Networks: Architectures And Protocols,* Prentice Hall.

Natarajan, K. and Mahadevan, G., 2013. A Succinct Comparative Analysis And Performance Evaluation Of Manet Routing Protocols. Computer Communication And Informatics (ICCCI), 2013 International Conference On, 2013. IEEE, 1-6.

Rafsanjani, M. K., Movaghar, A. and Koroupi, F., 2008. Investigating Intrusion Detection Systems In Manet And Comparing Idss For Detecting Misbehaving Nodes. *World Academy Of Science, Engineering And Technology,* 44**,** 351-355.

Raj, P. N. and Swadas, P. B., 2009. Dpraodv: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet. *Arxiv Preprint Arxiv:0909.2371*.

Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J. and Nygard, K. E., 2003. Prevention Of Cooperative Black Hole Attack In Wireless Ad Hoc Networks. International Conference On Wireless Networks, 2003.

Ros, F. J. and Ruiz, M., 2004. Implementing A New Manet Unicast Routing Protocol In Ns2. *Sun Microsystems Inc*.

Ruzgar, E. and Dagdeviren, O., 2013. Performance Evaluation Of Distributed Synchronous Greedy Graph Coloring Algorithms On Wireless Ad Hoc And Sensor Networks. *International Journal*.

Saha, H. N., Bhattacharyya, D., Banerjee, P., Bhattacharyya, A., Banerjee, A. and Bose, D., 2012. Study Of Different Attacks In Manet With Its Detection and Mitigation Schemes.

Sen, J., 2013. Detection Of Cooperative Black Hole Attack In Wireless Ad Hoc Networks. *Arxiv Preprint Arxiv:1302.4882*.

Shanthi, N., Lganesan, D. and Ramar, D. K., 2009. Study Of Different Attacks On Multicast Mobile Ad-Hoc Network. *Journal Of Theoretical And Applied Information Technology*, 9**,** 45-51.

Sharma, S. and Gupta, R., 2009. Simulation Study Of Blackhole Attack In The Mobile Ad Hoc Networks. *Journal Of Engineering Science And Technology*, 4**,** 243-250.

Singh, P. K. and Sharma, G., 2012. An Efficient Prevention Of Black Hole Problem In Aodv Routing Protocol In Manet. Trust, Security And Privacy In Computing And Communications (Trustcom), 2012 IEEE 11th International Conference On, 2012. IEEE, 902-906.

Singh, T. P., Dua, S. and Das, V., 2012. Energy-Efficient Routing Protocols In Mobile Ad-Hoc Networks. *International Journal Of Advanced Research In Computer Science And Software Engineering*, 5.

Srivastava, M., 2012. A Performance Analysis Of Routing Protocols In Mobile Ad-Hoc Networks. *International Journal Of Engineering*, 1.

Student, V. R. P. and Dhir, R., 2013. A Study Of Ad-Hoc Network: A Review. *International Journal*, 3.

Sun, B., Guan, Y., Chen, J. and Pooch, U. W., 2003. Detecting Black-Hole Attack In Mobile Ad Hoc Networks. Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492), 2003. Iet, 490-495.

Tamilselvan, L. and Sankaranarayanan, V., 2006. Solution To Prevent Rushing Attack In Wireless Mobile Ad Hoc Networks. Ad Hoc And Ubiquitous Computing, 2006. Isauhc'06. International Symposium On, 2006. IEEE, 42-47.

Tamilselvan, L. and Sankaranarayanan, V., 2008. Prevention Of Co-Operative Black Hole Attack In Manet. *Journal Of Networks,* 3**,** 13-20.

Ullah, I. and Rehman, S. U., 2010. Analysis Of Black Hole Attack On Manets Using Different Manet Routing Protocols. *A Mater Thesis, Electrical Engineering, Thesis No. Mee,* 10**,** 62.

Usha, U. and Bose, B., 2012. Comparing The Impact Of Black Hole And Gray Hole Attacks In Mobile Adhoc Networks. *Journal Of Computer Science,* 8**,** 2012.

Vincent, S. S. M. and Meshach, W. T., 2012. Preventing Black Hole Attack In Manets Using Randomized Multipath Routing Algorithm.